IVXV raamistiku nõuded krüptosüsteemile

Eeldused krüptosüsteemile

IVXV raamistik eeldab, et hääle salajasuse kaitsmiseks kasutatakse avaliku võtme krüptosüsteemi, millel on mitte-deterministlikkuse ja homomorfsuse omadused.

Avaliku võtme krüptosüsteem Defineerime krüptosüsteemi kui algoritmide kolmiku

$$\varepsilon = (G_{enc}, E, D),$$

kus G_{enc} on võtmegenereerimisalgoritm, E on krüpteerimisalgoritm ning D on dekrüpteerimisalgoritm. Edasises huvitavad meid asümmeetrilised ehk avaliku võtme krüptosüsteemid.

Avaliku võtme krüptosüsteemi võtmegenereerimisalgoritm G_{enc} väljastab kahest komponendist – avalikust võtmest ja privaatvõtmest – koosneva võtmepaari

$$k = (k_{pub}, k_{priv}) \in K$$

Krüptogrammi $c \in C$, mis on saadud avateksti $m \in M$ krüpteerimisel avaliku võtmega k_{pub}, on võimalik dekrüpteerida ainult privaatvõtmega k_{priv}, mis tagab ligipääsu avatekstile vaid privaatvõtme valdajale

$$\begin{aligned} c &= E(m, k_{pub}), \\ m &= D(c, k_{priv}). \end{aligned}$$

Mitte-deterministlikkuse omadus I-hääletamine eeldab hääle salajasuse tagamiseks kasutatavalt avaliku võtme krüptosüsteemilt mitte-deterministlikkuse omadust. Deterministlikuks nimetame krüptosüsteemi, mis kujutab sama võtme kasutamisel sama sõnumi alati samaks krüptogrammiks. Krüptosüsteemi deterministlikkus tähendab et kahe erineva valija poolt samale kandidaadile antud e-hääled on välisel vaatlusel identsed. Mitte-deterministlik krüptosüsteem kasutab krüpteerimisel juhuslikkust ning sama võtme k_{pub} kasutamisel kujutatakse sama sõnum m alati erinevaks krüptogrammiks c_i, eeldusel et krüpteerimisel kasutatav juhuslikkus r_i oli samuti erinev.

$$\begin{aligned} c_1 &= E(m, r_1, k_{pub}) \\ c_2 &= E(m, r_2, k_{pub}) \\ m_1 &= D(c_1, k_{priv}) \\ m_2 &= D(c_2, k_{priv}) \\ c_1 \neq c_2 &\iff r_1 \neq r_2 \\ m &= m_1 = m_2 \end{aligned}$$

Homomorfsuse omadus I-hääletamine eeldab hääle salajasuse tagamiseks kasutatavalt avaliku võtme krüptosüsteemilt homomorfsuse omadust, mis võimaldab teatud operatsioonide sooritamist krüptogrammidel ilma dekrüpteerimata.

Avaliku võtme krüptosüsteem ε on homomorfne n-aarse ($n \in \mathbb{N}$) funktsiooni f suhtes kui peab paika väide

$$\forall (k_{pub}, k_{priv}) \in K, \forall m_i \in M, i = 1, \ldots, n$$
$$f(E(m_1, k_{pub}), \ldots, E(m_n, k_{pub})) = E(f(m_1, \ldots, m_n), k_{pub})$$

I-hääletamise korral kasutatakse homomorfsuse omadust mitte-deterministliku krüptosüsteemiga krüpteeritud hääle ümberjuhulikustamiseks – krüptogrammis sisalduv juhuarv muudetakse teiseks juhuarvuks, jättes samas krüpteeritud sõnumi puutumata. Olgu algne krüptogramm

$$c_1 = E(m, r, k_{pub})$$

siis eeldades krüptosüsteemi homomorfsust funktsiooni $\cdot$ suhtes ning ühikelemendi 1 olemasolu saame ümberjuhulikustatud krüptogrammi

$$c_2 = E(m, r, k_{pub}) \cdot E(1, s, k_{pub}) = E(m \cdot 1, r \cdot s, k_{pub}) = E(m, r \cdot s, k_{pub})$$

Kehtivad järgmised võrdused

$$c_1 \neq c_2$$
$$m_1 = D(c_1, k_{priv})$$
$$m_2 = D(c_2, k_{priv})$$
$$m = m_1 = m_2$$

Ümberjuhulikustamise korrektsust peab olema võimalik tõestada osapoolele, kes ei kontrolli privaatvõtit.

ElGamal Toome näitena ElGamali avaliku võtme krüptosüsteemi [1], mis on mitte-deterministlik ja homomorfne krüptogrammide korrutamise suhtes.

ElGamali krüptosüsteem töötab multiplikatiivse rühma – näiteks $\mathbb{Z}_p^*$ – elementidel.

ElGamali süsteemi privaatvõti koosneb kolmest komponendist (p, g, z), kus

- p on suur algarv,
- $g \in \mathbb{Z}_p^*$ on rühma $\mathbb{Z}_p^*$ moodustaja,
- $z \leftarrow 2, \ldots, p-2$ on juhuslikult valitud arv.

ElGamali süsteemi avalik võti koosneb kolmest komponendist (g, p, y), kus

- $y = g^z \bmod p$.

Avaliku võtme (g, p, y), sõnumi $m \leftarrow 0, \ldots, p-1$ ja juhuarvu $r \leftarrow 2, \ldots, p-2$ korral toimub krüpteerimine järgmiselt:

$$c = (c_1, c_2) = (g^r \bmod p, m \cdot y^r \bmod p).$$

Krüptogrammi (c_1, c_2) ja privaatvõtme (p, g, z) korral dekrüpteeritakse sõnum m järgmiselt:

$$m = c_2 \cdot c_1^{-z}.$$

ElGamal krüptosüsteem on homomorfne krüptogrammide korrutamise suhtes. Olgu meil kaks ElGamali krüptosüsteemi krüptogrammi:

$$c_i = (g^r, m_1 \cdot y^r),$$
$$c_j = (g^s, m_2 \cdot y^s).$$

Osutub, et ka nende korrutis on korrektne krüptogramm:

$$c = c_i \cdot c_j = (g^r, m_1 \cdot y^r) \cdot (g^s, m_2 \cdot y^s) = (g^{r+s}, m_1 \cdot m_2 \cdot y^{r+s}).$$

Kokkuvõte Vajalike omadustega krüptosüsteemidest on ElGamal tuntuim ning läbiuurituim.

Levinuim viis ElGamali implementeerimiseks on täisarvujäägikorpustel, sellisel juhul on turvalised võtmepikkused samaväärsed tuntud RSA krüptosüsteemi võtmepikkustega.

ElGamali on võimalik implementeerida ka elliptkõveratel, sellisel juhul tuleks võrdlusaluseks võtta P-384 kõvera turvalisus.

Lugemistõend

Lugemistõendiks nimetame tõestust, et konkreetne e-hääl on dekrüpteeritud korrektselt. Lugemistõendeid kontrollides on võimalik veenduda, et hääletamistulemus on arvutatud korrektselt.

ElGamali krüptosüsteemi kasutamisel on lugemistõend realiseeritav, kasutades Schnorri nullteadmustõestusel põhinevat protokolli diskreetse logaritmi teadmise tõestamiseks [2].

Olgu meil räsifunktsioon h ning krüptogramm

$$c = (c_1, c_2) = (g^r \bmod p, m \cdot y^r \bmod p).$$

Dekrüpteerimine koos lugemistõendi väljastamisega toimub järgmiselt:

1. Dekrüpteerime krüptogrammi $d = c_1 c_2^{-x}$.
2. Valime t juhuslikult ning arvutame tõestuse esimese komponendi $a = c_2^t$.
3. Arvutame räsifunktsiooni h kasutades $k = h(a)$.
4. Arvutame tõestuse teise komponendi $s = kx + t$.
5. Väljastame avateksti d ning lugemistõendi komponendid a, s.

Lugemistõendi kontrollimiseks toimib audiitor järgmiselt:

1. Arvutab k lugemistõendi esimese komponendi põhjal $k = h(a)$.
2. Kontrollib võrdust $c_2^s = a(c_1/d)^k$.

Kirjeldatud viis on levinud ja läbiuuritud lähenemine lugemistõendi koostamiseks ElGamal krüptosüsteemi korral. Alternatiivsete lähenemiste korral tuleks koos algoritmiga esitada tõestus algoritmi korrektsuse ning nullteadmuse kohta.

E-häälte anonüümimine miksimise teel

IVXV raamistik näeb ette võimaluse täiendava anonüümimismeetodi – krüptograafilise miksimise – kasutamiseks. Krüptograafiline miksimine on protsess, mis võtab sisendiks hulga krüpteeritud hääli B_1 ja annab väljundiks hulga krüpteeritud hääli B_2 ning miksimistõendi P_{mix} selliselt, et:

1. B_1 ja B_2 dekrüpteerimisel tekkivad avatekstide hulgad on samad;
2. ühegi krüpteeritud hääle kohta hulgast B_2 ei ole võimalik öelda, milline krüpteeritud hääl hulgast B_1 on temaga vastavuses ja vastupidi;
3. P_{mix} on matemaatiline tõestus tingimuse 1 täidetuse kontrollimiseks. P_{mix} kontrollimine on võimalik ilma hulkade B_1 ja B_2 vahelist vastavust avaldamata.

Sisuliselt tähendab krüptograafiline miksimine seda, et algsete krüpteeritud häälte asemel võime avada miksitud hääled, arvutada hääletamistulemuse ning kontrollida miksitud häälte dekrüpteerimisel saadud lugemistõendit. Kui saame kontrollida, et miksimisprotsessi sisendiks läksid õiged hääled, siis võime kogu protsessi lõpuks olla veendunud, et hääletamistulemus arvutati sisendist lähtudes korrektselt. Tänu miksimisele saab audiitor veenduda tulemuse korrektsuses, kuid ei saa mingit informatsiooni konkreetsete valijate eelistuste kohta.

Krüptograafilise miksimise rakendamine nõuab kasutatavalt krüptosüsteemilt ümberjuhulikustamise võimalust homomorfsuse omadust kasutades. Ümberjuhulikustamise tulemusena saame kaks krüptogrammi, mille krüpteeritud sõnum on identne, kuid esitusviis erinev. Tõestus korrektsest ümberjuhulikustamisest on osa miksimistõendist.

Täitmaks krüptograafilisele miksimisele seatavat nõuet – vastavus sisendi ja väljundi vahel peab olema peidetud – rakendatakse miksimisel lisaks ümberjuhulikustamisele ka segamist, mille tulemusena esitab miksimisprotsess oma väljundiks ümberjuhulikustatud sisendkrüptogrammid teises järjekorras.

Miksimistõend on terviktõestus, mis näitab, et väljundhäälte hulk on saadud sisendhäälte hulgast korrektse ümberjuhulikustamise ja segamise teel. Tõestus antakse nullteadmuse abil, mis tähendab, et me saame kinnituse väite paikapidavusest, kuid miksimisprotsessi siseinfot meile ei avalikustata. Kui lugemistõend antakse iga avatud hääle kohta eraldi, siis miksimistõend on alati üks tervik sõltumata miksitud häälte hulgast.

Kasutatav miksimismeetod peab olema ühilduv lugemistõendi saavutamiseks kasutatava krüptosüsteemiga, miksimise rakendamine või mitterakendamine ei tohi mõjutada häälte dekrüpteerimist ega lugemistõendite koostamist ning auditeerimist. Miksimismeetodi poolt kasutatav miksimistõendi algoritm peab olema tõestatavalt turvaline.

Viited

1. Taher El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc.
2. Claus-Peter Schnorr. Efficient Identification and Signatures for Smart Cards. In Gilles Brassard, editor, *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer, 1989.